WHAT IS CLAIMED IS:

1. An architecture for delivery of communications services within a hospital, comprising:
   - a set of healthcare data processing resources for providing healthcare communications services to users at a plurality of delivery points throughout the hospital;
   - a set of non-healthcare data processing resources for providing non-healthcare communications services to the users at the plurality of delivery points;
   - a data routing entity connected to the healthcare data processing resources and to the non-healthcare data processing resources;
   - a common access infrastructure connected between the data routing entity and the plurality of delivery points, for supporting both the healthcare communications services and the non-healthcare communications services;
   - the data routing entity being operative to control access by the users at the plurality of delivery points to the healthcare data processing resources and to the non-healthcare data processing resources.

2. The architecture defined in claim **1**, wherein the healthcare communications services and the non-healthcare communications services delivered to a common one of the delivery points occupy the common access infrastructure during mutually exclusive periods of time.

3. The architecture defined in claim **1**, wherein the healthcare communications services and the non-healthcare communications services delivered to a common one of the delivery points occupy the common access infrastructure contemporaneously.

4. The architecture defined in claim **3**, wherein the healthcare communications services and the non-healthcare communications services delivered to a common one of the plurality of delivery points are delivered over distinct logical connections sharing the common access infrastructure.

5. The architecture defined in claim **1**, wherein, at a given time instant, healthcare communications services are being delivered to a first subset of the plurality of

delivery points while non-healthcare communications services are being delivered to a second subset of the plurality of delivery points.

6. The architecture defined in claim **1**, wherein the healthcare data processing resources comprise a plurality of healthcare application servers for running clinical software.

7. The architecture defined in claim **6**, wherein the healthcare communications services comprise a computerized physician order entry service.

8. The architecture defined in claim **1**, wherein the healthcare data processing resources comprise a healthcare authentication entity for authenticating users at the delivery points claiming to be healthcare users.

9. The architecture defined in claim **8**, wherein the non-healthcare data processing resources comprise a non-healthcare authentication entity for authenticating users of the delivery points claiming to be non-healthcare users.

10. The architecture of claim **9**, the data routing entity further comprising an access controller operative to:
    - receive an authentication request message comprising user credentials and a user class regarding a user at a given one of the plurality of delivery points;
    - determine, based on the user class, a destination authentication entity from between the healthcare authentication and the non-healthcare authentication entity;
    - release the user credentials towards the destination authentication entity for authentication of the user.

11. The architecture defined in claim **10**, the access controller further operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

12. The architecture defined in claim **11**, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the delivery of a healthcare

communications service from the healthcare data processing resources or a non-healthcare communications service from the non-healthcare data processing resources, in dependence upon the user class corresponding to the user.

13. The architecture defined in claim **11**, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

14. The architecture defined in claim **13**, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the delivery of either a healthcare communications service if the user is determined to belong to the healthcare user class, or a non-healthcare communications service if the user is determined to belong to the non-healthcare user class.

15. The architecture defined in claim **14**, the data routing entity further comprising a switching entity operative to route the authentication request message to the access controller.

16. The architecture defined in claim **15**, the data routing entity further comprising a second switching entity for selective establishment of connections between the delivery point and either the healthcare data processing resources or the non-healthcare data processing resources.

17. The architecture defined in claim **16**, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by providing an indication of said successful authentication of the user by the destination authentication entity to a second one of the authentication entities other than the destination authentication entity.

18. The architecture defined in claim **17**, the second authentication entity being operative to prevent establishment of a connection for the exchange of data between the delivery

point and a subset of the data processing resources other than the subset of the data processing resources with which a connection has been established.

19. The architecture defined in claim **18**, wherein the second authentication entity being operative to prevent establishment of a connection comprises the second authentication entity causing the second switching entity to deny any connections therethrough which would allow establishment a connection between the end user device and said subset of the data processing resources other than the subset of the data processing resources with which a connection has been established.

20. The architecture defined in claim **1**, wherein the non-healthcare data processing resources comprise a digital entertainment head end for controlling delivery to the delivery points of received digital entertainment services.

21. The architecture defined in claim **20**, wherein the non-healthcare communications services comprise patient entertainment services.

22. The architecture defined in claim **21**, wherein the non-healthcare communications services comprise personal video recorder services.

23. The architecture defined in claim **1**, wherein the non-healthcare data processing resources comprise an Internet gateway.

24. The architecture defined in claim **1**, wherein the non-healthcare data processing resources comprise a patient information server for allowing access to patient information services.

25. The architecture defined in claim **1**, wherein the data routing entity is operative to permit delivery of non-healthcare communications services to a first one of the delivery points in response to successful authentication of a user at said first delivery point claiming to be a non-healthcare user.

26. The architecture defined in claim **1**, wherein the data routing entity is operative to permit delivery of healthcare communications services to a first one of the delivery points in response to successful authentication of a user at said first delivery point claiming to be a healthcare user.

27. The architecture defined in claim **26**, wherein the data routing entity is operative to permit delivery of non-healthcare communications services to said first delivery point in response to successful authentication of a user at said first delivery point claiming to be a non-healthcare user.

28. The architecture defined in claim **27**, wherein a healthcare user is defined as a user who is a physician, a nurse or an orderly.

29. The architecture defined in claim **28**, wherein a non-healthcare user is defined as a user who is an admitted patient or a visitor.

30. The architecture defined in claim **1**, wherein the access infrastructure comprises a partly wireless infrastructure.

31. The architecture defined in claim **1**, wherein the access infrastructure comprises a fixed-wire cabling infrastructure.

32. The architecture defined in claim **1**, wherein the fixed-wire cabling infrastructure comprises point-to-point telephony wiring.

33. The architecture defined in claim **31**, wherein the cabling infrastructure includes a twisted pair wiring base.

34. The architecture defined in claim **33**, wherein said twisted pair wiring base comprises PBX access-side twisted pair.

35. The architecture defined in claim **33**, wherein said twisted pair wiring base comprises Cat 2-3 twisted pair.

36. The architecture defined in claim **33**, wherein said twisted pair wiring base comprises Cat 5 twisted pair.

37. The architecture defined in claim **1**, further comprising:
    - a telephony head end connected to the access infrastructure and operative to exchange telephony signals via the access infrastructure used to support both the healthcare communications services and the non-healthcare communications services.

38. The architecture defined in claim **37**, wherein the telephony signals are digital telephony signals.

39. The architecture defined in claim **38**, wherein the telephony signals occupy a first frequency range and wherein the healthcare communications services and the non-healthcare communications services occupy a second frequency range different from the first frequency range.

40. The architecture defined in claim **39**, wherein the first frequency range is lower than the first frequency range.

41. The architecture defined in claim **37**, wherein the telephony signals are baseband analog telephony signals.

42. An access controller for use in authenticating users of a network, the access controller comprising:
    - an input operative to receive an authentication request message indicative of user credentials and a user class regarding a user of an end user device;
    - a control entity operative to determine, based on the user class, a destination authentication entity from among a plurality of authentication entities;
    - an output operative to release the user credentials towards the destination authentication entity for authentication of the user.

43. The access controller defined in claim **42**, further comprising a second input operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

44. The access controller defined in claim **43**, the control entity being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the exchange of data between the end user device and a subset of the data processing resources.

45. The access controller defined in claim **44**, the second input further operative to receive from the destination authentication entity an access profile indicative of the subset of the data processing resources.

46. The access controller defined in claim **45**, the control entity being further operative to respond to successful authentication of the user by the destination authentication entity by preventing establishment of a connection for the exchange of data between the end user device and a predetermined second subset of the data processing resources.

47. The access controller defined in claim **42**, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

48. A host processing entity for use in allowing users to access data processing resources in a hospital, the host processing entity comprising:
    - a plurality of authentication entities for authenticating users belonging to respective user classes;
    - an access controller operative to:
        - receive an authentication request message comprising user credentials and a user class regarding a user at an end user device;
        - determine, based on the user class, a destination authentication entity from among the plurality of authentication entities;
        - release the user credentials towards the destination authentication entity for authentication of the user.

49. The host processing entity defined in claim **48**, the access controller further operative to receive from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

50. The host processing entity defined in claim **49**, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by causing establishment of a connection for the exchange of data between the end user device and a subset of the data processing resources.

51. The host processing entity defined in claim **50**, the access controller being further operative to receive from the destination authentication entity an access profile indicative of the subset of the data processing resources.

52. The host processing entity defined in claim **51**, further comprising a switching entity operative to establish the connection between the end user device and the subset of the data processing resources.

53. The host processing entity defined in claim **51**, the access controller being further operative to respond to successful authentication of the user by the destination authentication entity by providing an indication of said successful authentication of the user by the destination authentication entity to a second one of the authentication entities other than the destination authentication entity.

54. The host processing entity defined in claim **53**, the second authentication entity being operative to prevent establishment of a connection for the exchange of data between the end user device and a second subset of the data processing resources other than the first subset of the data processing resources.

55. The host processing entity defined in claim **54**, further comprising a switching entity operative to establish the connection between the end user device and the first subset of the data processing resources.

56. The host processing entity defined in claim **55**, wherein the second authentication entity being operative to prevent establishment of a connection comprises the second authentication entity causing the switching entity to deny any connections therethrough which would allow establishment a connection between the end user device and the second subset of the data processing resources.

57. The host processing entity defined in claim **48**, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

58. A method of controlling user access to resources in a data network, the method comprising:
- receiving an authentication request message comprising user credentials and a user class regarding a user at an end user device;
- determining, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- releasing the user credentials towards the destination authentication entity for authentication of the user.

59. The method defined in claim **58**, further comprising:
- receiving from the destination authentication entity an indication of successful or unsuccessful authentication of the user by the destination authentication entity.

60. The method defined in claim **59**, further comprising:
- responsive to successful authentication of the user by the destination authentication entity, enabling the user to access a subset of the resources in the data network that depends on the user class corresponding to the user.

61. The method defined in claim **60**, the subset of the resources in the data network being a first subset of the resources in the data network, the method further comprising:
- responsive to successful authentication of the user by the destination authentication entity, disabling the user from accessing a second subset of the resources in the data network that depends on the user class corresponding to the user.

62. The method defined in claim **61**, wherein the user class corresponding to the user belongs to a set comprising at least a healthcare user class and a non-healthcare user class.

63. The method defined in claim **62**, wherein the first subset of the resources in the data network comprises patient entertainment and information systems when the user class corresponding to the user is the non-healthcare user class.

64. The method defined in claim **63**, wherein the first subset of the resources in the data network comprises healthcare application servers when the user class corresponding to the user is the healthcare user class.

65. The method defined in claim **60**, further comprising:
- receiving from the destination authentication entity an indication of the first subset of the resources in the data network.

66. The method defined in claim **65**, wherein enabling the user to access the first subset of the resources in the data network comprises enabling the establishment of a session between the remote entity and the first subset of the resources in the data network.

67. The method defined in claim **66**, further comprising, in the case of successful authentication of the user by the destination authentication entity:
- receiving from the destination authentication entity an indication of the second set of the resources in the data network.

68. The method defined in claim **67**, wherein disabling the user from accessing the second subset of the resources in the data network comprises disabling the establishment of a session between the remote entity and the second subset of the resources in the data network.

69. The method defined in claim **66**, further comprising, in the case of successful authentication of the user by the destination authentication entity:

- providing an indication of said successful authentication of the user by the destination authentication entity to an authentication entity other than the destination authentication entity.

70. The method defined in claim **69**, further comprising:
    - receiving from said authentication entity other than the destination authentication entity an indication of the second set of the resources in the data network.

71. The method defined in claim **66**, wherein the first and second subsets of the resources in the data network each comprise respective interfaces of a data switching entity.

72. The method defined in claim **71**, wherein said interfaces comprise physical ports of the data switching entity.

73. The method defined in claim **71**, wherein said interfaces comprise logical connections through the data switching entity.

74. The method defined in claim **48**, wherein releasing the user credentials towards the destination authentication entity comprises not releasing the user credentials towards any authentication entity other than the destination authentication entity.

75. The method defined in claim **48**, further comprising:
    - responsive to successful authentication of the user by the destination authentication entity, providing a command to enable a set of resources in the end user device.

76. The method defined in claim **48**, further comprising:
    - responsive to unsuccessful authentication of the user by the destination authentication entity, providing a command to disable a set of resources in the end user device.

77. The method defined in claim **56**, the session being a first session, the destination authentication entity being the first authentication entity, the method further comprising:

- during the first session, receiving a second authentication request message indicative of second user credentials and a second user class regarding a second user at the end user device;
- determining, based on the second user class, a second destination authentication entity from among the plurality of authentication entities;
- releasing the second user credentials towards the second destination authentication entity for authentication of the second user.

78. The method defined in claim **77**, further comprising:
- suspending the first session.

79. The method defined in claim **78**, wherein suspending the first session is performed prior to determining the second destination authentication entity.

80. The method defined in claim **79**, wherein suspending the first session comprises:
- if the first session corresponds to delivery of a video stream to the remote device, routing the video stream to a personal video recorder for future access by the first user.

81. The method defined in claim **79**, wherein suspending the first session comprises:
- if the first session corresponds to an electronic mail application, saving a context of the electronic mail application for future retrieval by the first user.

82. Computer-readable media tangibly embodying a program element for execution by a computing device to implement an access controller, said access controller including:
- an interface entity operative to receive an authentication request message indicative of user credentials and a user class regarding a user at an end user device;
- a control entity operative to determine, based on the user class, a destination authentication entity from among a plurality of authentication entities;
- the interface further operative to release the user credentials towards the destination authentication entity for authentication of the user.

83. An access controller for controlling user access to resources in a data network, comprising:
    - means for receiving an authentication request message indicative of user credentials and a user class regarding a user at an end user device;
    - means for determining, based on the user class, a destination authentication entity from among a plurality of authentication entities;
    - means for releasing the user credentials towards the destination authentication entity for authentication of the user.

84. A method of formulating an authentication request message, comprising:
    - receiving authentication primitives from an end user, the authentication primitives being indicative of a user class and user credentials regarding a user;
    - determining the user class from the authentication primitives;
    - creating an authentication request message from the authentication primitives, the authentication request message containing data indicative of at least the user credentials and being in a format that is dependent upon the user class;
    - outputting the authentication request message.

85. The method defined in claim **84**, further comprising:
    - validating the authentication primitives to determine compliance with a predetermined format;
    - wherein creating is conditional upon the authentication primitives complying with the predetermined format.

86. The method defined in claim **85**, wherein the predetermined format comprises a first portion that encodes the user class.

87. The method defined in claim **86**, wherein the predetermined format comprises a second portion that encodes user credentials comprising a user identity and corroborating evidence.

88. The method defined in claim **87**, wherein said first portion comprises data supplied by a bar code reader or magnetic card reader.

89. The method defined in claim **87**, wherein said first portion and said user identity comprises data supplied by a bar code reader or magnetic card reader.

90. The method defined in claim **87**, wherein the corroborating evidence comprises biometric data obtained from the user.

91. The method defined in claim **87**, wherein the user identity comprises a user name and wherein the corroborating evidence comprises a personal identification code.

92. An end user device, comprising:
- an input device operative to receive authentication primitives from an end user, the authentication primitives being indicative of a user class and user credentials regarding a user;
- a message formulator, operative to determine the user class from the authentication primitives and to create an authentication request message from the authentication primitives, the authentication request message containing data indicative of at least the user credentials and being in a format that is dependent upon the user class;
- an output for releasing the authentication request message.

93. The end user device defined in claim **92**, wherein the input device comprises an authentication device.

94. The end user device defined in claim **93**, wherein the authentication device comprises at least one of a bar code scanner, a biometric reader, a magnetic card reader and a radio frequency badge reader.

95. The end user device defined in claim **92**, further comprising a main processor that is capable of receiving data from the message formulator and prevented from sending data to the message formulator.